On Kummer Lines with Full Rational 2-torsion and Their Usage in Cryptography

HUSEYIN HISIL, Yasar University, Turkey
JOOST RENES, Radboud University, The Netherlands

A paper by Karati and Sarkar at Asiacrypt'17 has pointed out the potential for Kummer lines in genus 1, by observing that their SIMD-friendly arithmetic is competitive with the status quo. A more recent preprint explores the connection with (twisted) Edwards curves. In this article, we extend this work and significantly simplify the treatment of Karati and Sarkar. We show that their Kummer line is the x-line of a Montgomery curve translated by a point of order two, and exhibit a natural isomorphism to the y-line of a twisted Edwards curve. Moreover, we show that the Kummer line presented by Gaudry and Lubicz can be obtained via the action of a point of order two on the y-line of an Edwards curve. The maps connecting these curves and lines are all very simple. As a result, a cryptographic implementation can use the arithmetic that is optimal for its instruction set at negligible cost.

CCS Concepts: • **Security and privacy → Cryptography**; **Public key encryption**;

Additional Key Words and Phrases: Montgomery curves, Edwards curves, Kummer lines, Montgomery ladder, digital signatures

ACM Reference format:
Huseyin Hisil and Joost Renes. 2019. On Kummer Lines with Full Rational 2-torsion and Their Usage in Cryptography. *ACM Trans. Math. Softw.* 45, 4, Article 39 (December 2019), 17 pages.
https://doi.org/10.1145/3361680

1 INTRODUCTION

A decade after the introduction of public-key cryptography by Diffie and Hellman [1976] it was observed (independently) by Miller [1986] and Koblitz [1987] that one can instantiate protocols based on the hardness of the discrete logarithm problem with the group of rational points of an elliptic curve E defined over a finite field. Moreover, it was immediately noted by Miller that one can do a full key exchange by solely relying on the line of x-coordinates of points. That is, one can identify points with their inverses and as a result only work with points up to sign. In other words, one can work on the corresponding Kummer line $K = E/\{\pm 1\}$, possibly simplifying the arithmetic. Recently it was shown that one can also directly use K for digital signatures very efficiently with the qDSA scheme [Renes and Smith 2017, Section 12]. Similar properties hold for Jacobians of

The second author is partially supported by the Technology Foundation STW (project 13499—TYPHOON & ASPASIA), from the Dutch government.
Authors' addresses: H. Hisil, Yasar University, Selcuk Yasar Campus, Room U110, Engineering Faculty, Computer Engineering Department, Universite Caddesi, No 35-37, Agacli Yol, Bornova, Izmir, 35100, Turkey; email: huseyin.hisil@yasar.edu.tr; J. Renes, Radboud University, Room 3.11, Faculty of Science, University of Nijmegen, Postbus 9010, 6500GL, Nijmegen, The Netherland; email: j.renes@cs.ru.nl.

0098-3500/2019/12-ART39 $15.00
https://doi.org/10.1145/3361680

higher genus curves and their Kummer varieties, leading to especially pleasing formulas [Gaudry 2007] and very efficient implementations [Bernstein et al. 2014] in the case of genus 2, though we do not consider those here. In short, Kummer lines are a very interesting topic of study from a cryptographic perspective.

Because a reduction in the number of field operations needed for a scalar multiplication directly affects the efficiency of the cryptographic scheme, there have been multiple proposals for Kummer lines. Probably the most popular example is Curve25519 [Bernstein 2006a], which is the Kummer line of a Montgomery curve. One can show that every Montgomery curve is birationally equivalent to a twisted Edwards curve [Bernstein et al. 2008, Theorem 3.2], which currently needs the least number of field operations to perform group operations [Hisil et al. 2008] and underlies the very efficient Four$\mathbb{Q}$ curve [Costello and Longa 2015]. As a result, the Kummer lines of Montgomery and twisted Edwards curves are strongly related, and one can move easily from one to the other [Bernstein et al. 2008; Castryck et al. 2008]. Through the usage of theta functions Gaudry and Lubicz [2009, Section 6] derived yet another Kummer line. We shall refer to this as the *canonical* Kummer line, following the terminology of the genus 2 analogue presented by Renes and Smith [2017, Section 4]. By squaring its coefficients, we arrive on a different variety, which we refer to as the *squared* Kummer line (again, cf. the genus 2 analogue [Bernstein 2006b; Chudnovsky and Chudnovsky 1986]). Although Gaudry and Lubicz only presented arithmetic on the canonical line, the differential addition formulae on the squared Kummer line are well-known [Bernstein and Lange 2015]. The squared Kummer line has the advantage that it is easier to find suitable small parameters, and it was shown by Karati and Sarkar [2017b] that its arithmetic leads to very efficient implementations when single-instruction multiple-data (SIMD) instructions are available.

In a follow-up paper [Karati and Sarkar 2017a] the same authors present connections to twisted Edwards curves. This requires the associated Legendre curve to be put in Montgomery form or have a rational point of order 4, or otherwise relies on the usage of a 2-isogeny. Consequently, there are case distinctions and one must deal with the doubling induced by moving through a 2-isogeny and its dual. In Karati and Sarkar [2017a], Table 7 they present the possibility of birational maps and isogenies between the Legendre form for certain choices of small constants.

In this article, we significantly simplify the connections between the various Kummer lines. Since the field of definition of the curves under consideration, i.e., those from which the canonical and squared Kummer lines arise, corresponds to the field of definition of its 2-torsion, we shall assume all points of order 2 to be rational over the base field (see also Remark 3). In that case, we show that the squared (respectively, canonical) Kummer arises as the x-line (respectively, y-line) of a Montgomery (respectively, Edwards) curve translated by a suitable point of order 2. Moreover, a third Kummer line (referred to as the *intermediate* Kummer) appears as the y-line of a *twisted* Edwards curve via a translation by a point of order 2. These observations induce very simple isomorphisms between them. Furthermore, the respective translations by a point of order 2 lead to fast isomorphisms (in fact, involutions) with the well-known x-lines (or y-lines) of Montgomery, Edwards, and twisted Edwards curves. As a result, we unify the most popular Kummer lines in the literature and conclude that their usage is completely interchangeable on an implementation level. For example, we can directly use the squared Kummer line in the qDSA scheme through its connection with a Montgomery curve [Renes and Smith 2017, Section 3]. Moreover, although there exist efficient implementations of Montgomery curves based on 4-way SIMD parallelization by optimizing the field arithmetic [Faz-Hernández and López 2015], it is unclear how to optimally parallelize instructions 4-way on the level of the x-line [Chou 2015]. This is straightforward on the squared Kummer line, and therefore by extension becomes trivial on Montgomery curves with full rational 2-torsion by moving through the isomorphism. Of course, if desired, one can also do arithmetic on the full group of points of the twisted Edwards curve (as also noted by Karati and

Sarkar [2017a]). In particular, we provide isomorphic Montgomery and twisted Edwards models for all the Kummer lines present in Karati and Sarkar [2017a], Table 7 (see Table 1 in Section 3.2).

2 PRELIMINARIES

Let k be a field such that $\mathrm{char}(k) \neq 2$ (this assumption is implicit in the whole document). An elliptic curve is a smooth projective curve of genus 1 with a specified base point O, and it is said to be defined over k if E is defined over k and $O \in E(k)$ [Silverman 2009, Section III.3]. Its points form an abelian group with neutral element O. One can show [Silverman 2009, Proposition III.3.1] that any elliptic curve defined over k can be put in *Weierstrass form*[1]

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6,$$

with $O = (0 : 1 : 0)$, but the curves we consider in this article are not generally in this standard model. If we want to emphasize the base point of the curve we are working with, then we shall write (E, O).

Any such curve is a double cover of $\mathbb{P}^1$ via a (surjective) degree-2 projection map $\pi : E \to \mathbb{P}^1$ invariant under composition with $[\pm 1]$, which induces a bijection between $(E, O)/\{\pm 1\}$ and $\mathbb{P}^1$. For that reason, the projective line inherits a pseudo-group structure from (E, O) through π, and in particular we obtain a scalar multiplication on $\mathbb{P}^1$ as first used by Montgomery [1987, Section 10]. We denote the projective line with the induced pseudo-group structure of (E, O) by K_E^O, and refer to it as its Kummer line (see Sections 2.0.1–2.0.3 for some examples).

Morphisms $\overline{\phi} : K_1 \to K_2$ between any two Kummer lines K_1 and K_2 are defined to be maps of the form $\overline{\phi} = \pi_2\phi\pi_1^{-1}$, where $\pi_1 : (E_1, O_1) \to K_1$ and $\pi_2 : (E_2, O_2) \to K_2$ are the corresponding projection maps and $\phi : (E_1, O_1) \to (E_2, O_2)$ is a morphism of elliptic curves (i.e., an isogeny). Note that the pre-image under π_1 is not necessarily well-defined, but that the composition with $\pi_2\phi$ is. We say that $\overline{\phi}$ is an *isomorphism* whenever ϕ is, and call it an *involution* whenever it is an involution as a map $\mathbb{P}^1 \to \mathbb{P}^1$.

2.0.1 Montgomery Curves. Let $A, B \in k$ such that $B(A^2 - 4) \neq 0$ and let M/k be the smooth projective curve of genus 1 defined by the affine equation

$$By^2 = x^3 + Ax^2 + x.$$

We may write $M_{A,B}$ for M to emphasize the coefficients of the curve we are referring to. Denoting $O_M = (0 : 1 : 0)$, the elliptic curve (M, O_M) is commonly referred to as a *Montgomery curve* [Montgomery 1987] and is ubiquitous in elliptic-curve-based cryptography protocols (see, e.g., Bernstein [2006a]). The projection map to the Kummer line is given by projection onto the x-axis

$$\mathbf{x} : M \to \mathbb{P}^1$$
$$(X : Y : Z) \mapsto \begin{cases} (X : Z) & \text{if } Z \neq 0 \\ (1 : 0) & \text{if } Z = 0 \end{cases},$$

and we denote by $K_M^{O_M}$ the Kummer line.

Now suppose that $T \in (M, O_M)$ is a point such that $[2]T = O_M$. Then the translation-by-T map

$$\tau_T : (M, O_M) \to (M, T)$$
$$P \mapsto P + T$$

[1]We shall in many cases talk about *affine* curves and maps for simplicity, but always mean their projective counterparts. This depends on the particular embedding of the affine curve into projective space, but it should be clear from context what is meant. In particular, we always embed Montgomery curves into $\mathbb{P}^2$ while (twisted) Edwards curves are embedded into $\mathbb{P}^1 \times \mathbb{P}^1$.

is an isomorphism of elliptic curves. Moreover, the map $\mathbf{x}$ is again well-defined on $(M,T)/\{\pm 1\}$ and we denote its Kummer line by K_M^T. In summary, we have a commutative diagram

$$\begin{array}{ccc} (M,O_M) & \xleftrightarrow{\tau_T} & (M,T) \\ \downarrow \mathbf{x} & & \downarrow \mathbf{x} \\ K_M^{O_M} & \xleftrightarrow{\overline{\tau}_T} & K_M^T \end{array},$$

where $\overline{\tau}_T$ is the induced isomorphism (involution) between the corresponding Kummer lines. For example, we obtain the map $\overline{\tau}_{(0,0)} : (X:Z) \mapsto (Z:X)$. Since $\#(M,O_M)[2] = 4$, there are at most two other points of order 2. This gives rise to only a single non-trivial action on the Kummer line $K_M^{O_M}$, since the other is simply the composition with $\overline{\tau}_{(0,0)}$.

2.0.2 Twisted Edwards Curves. Let $\alpha, \delta \in k$ such that $\alpha\delta(\alpha - \delta) \neq 0$ and consider the smooth projective curve of genus 1 defined by the equation

$$\alpha x^2 + y^2 = 1 + \delta x^2 y^2.$$

This is commonly referred to as the *twisted Edwards* model [Bernstein et al. 2008], where the base point is chosen as $O = (0,1)$. It is closely related to a Montgomery curve via a birational map [Bernstein et al. 2008, Theorem 3.2(i)]. The naïve embedding into $\mathbb{P}^2$ has (nodal) singular points at infinity, so instead we consider its embedding into $\mathbb{P}^1 \times \mathbb{P}^1$ sending $(x,y) \mapsto ((x:1),(y:1))$ onto

$$E/k : \alpha X^2 T^2 + Y^2 Z^2 = Z^2 T^2 + \delta X^2 Y^2 \subset \mathbb{P}^1 \times \mathbb{P}^1. \tag{1}$$

This can be further embedded into $\mathbb{P}^3$ using the Segre embedding $((X:Z),(Y:T)) \mapsto (XY : XT : ZY : ZT)$, recovering the embedding from Hisil [2010], Section 2.3.4, or Galbraith [2012], Lemma 9.12.18. When referring to twisted Edwards curves, we will mean their embedding into $\mathbb{P}^1 \times \mathbb{P}^1$ conform to Equation (1) and may write $E_{\alpha,\delta}$ to emphasize its coefficients. Note that this is a purely theoretical tool, since once all is said and done the cryptographically relevant arithmetic is performed in a prime order subgroup in which all points are affine. For affine points, we will sometimes use the affine notation and expect that this should not cause confusion. On E there exist 4 points *at infinity*

$$\Omega^+ = ((1:0),(1:\sqrt{\delta/\alpha})), \qquad \Omega^- = ((1:0),(1:-\sqrt{\delta/\alpha})),$$
$$\omega^+ = ((1:\sqrt{\delta}),(1:0)), \qquad \omega^- = ((1:-\sqrt{\delta}),(1:0)),$$

where Ω^+, Ω^- have order 2 and ω^+, ω^- have order 4 on (E,O_E).

Similar to the $\mathbf{x}$-map for Montgomery curves arising as a projection onto the x-axis, we have a $\mathbf{y}$-map

$$\mathbf{y} : E \to \mathbb{P}^1$$
$$((X:Z),(Y:T)) \mapsto (Y:T),$$

corresponding to projection onto the y-axis. Since inversion in this case is negation of the x-coordinate, this map is well-defined on $(E,O_E)/\{\pm 1\}$ and we denote the Kummer line by $K_E^{O_E}$. The point $S = ((0:1),(-1:1))$ of order 2 induces the commutative diagram

$$\begin{array}{ccc} (E,O_E) & \xleftrightarrow{\tau_S} & (E,S) \\ \downarrow \mathbf{y} & & \downarrow \mathbf{y} \\ K_E^{O_E} & \xleftrightarrow{\overline{\tau}_S} & K_E^S \end{array}, \tag{2}$$

where $\overline{\tau}_S : (Y : Z) \mapsto (-Y : Z)$. The two other 2-torsion points induce one other non-trivial translation (analogous to the Montgomery model).

2.0.3 Edwards Curves. Let $c \in \bar{k}$ such that $c^5 \neq c$ and

$$\mathcal{E} : x^2 + y^2 = c^2(1 + x^2y^2),$$

again a smooth curve of genus 1. This is technically only a subset of the set of curves of the form $x^2 + y^2 = c^2(1 + dx^2y^2)$ originally defined as Edwards curves by Bernstein and Lange [2007]. But in this article, we only encounter the case $d = 1$, which corresponds to the form introduced by Edwards [2007], who observed that its arithmetic with respect to the base point $O_{\mathcal{E}} = (0, c)$ is extremely symmetric. As above, we use the smooth model inside $\mathbb{P}^1 \times \mathbb{P}^1$ containing the elements

$$\Theta^+ = ((1 : 0), (1 : c)), \qquad \Theta^- = ((1 : 0), (1 : -c)),$$
$$\theta^+ = ((1 : c), (1 : 0)), \qquad \theta^- = ((1 : -c), (1 : 0)),$$

where Θ^+, Θ^- (respectively, θ^+, θ^-) have order 2 (respectively, 4) on $(\mathcal{E}, O_{\mathcal{E}})$. Again, we have a projection to $\mathbb{P}^1$

$$\mathrm{y} : \mathcal{E} \to \mathbb{P}^1$$
$$((X : Z), (Y : T)) \mapsto (Y : T).$$

We denote the Kummer line of $(\mathcal{E}, O_{\mathcal{E}})$ obtained by projection through y by $K_{\mathcal{E}}^{O_{\mathcal{E}}}$. For any 2-torsion point R of $(\mathcal{E}, O_{\mathcal{E}})$, we obtain a commutative diagram as in (2) by translation by R and denote the Kummer line by $K_{\mathcal{E}}^{R}$.

2.0.4 Rationality and Quadratic Twists. Suppose that q is a prime power and $k = \mathbb{F}_q$ is a finite field. Then any elliptic curve E defined over $\mathbb{F}_q$ will have a quadratic twist, i.e., an elliptic curve E^t that is $\mathbb{F}_{q^2}$-isomorphic but not $\mathbb{F}_q$-isomorphic to E. This is unique up to $\mathbb{F}_q$-isomorphism (hence, why we talk about *the* quadratic twist). For example, any two Montgomery curves $M_{A,B}$ and $M_{A,B'}$ where B/B' is a non-square in $\mathbb{F}_q$ are quadratic twists. Given any non-square $u \in \mathbb{F}_q^*$, the curves

$$E^t : u\alpha x^2 + y^2 = 1 + u\delta x^2y^2, \quad \mathcal{E}^t : ux^2 + y^2 = c^2(1 + ux^2y^2)$$

are quadratic twists of (twisted) Edwards curves. Note that $\mathcal{E}^t$ is technically no longer an Edwards curve, but it is easy to see that its group law is similar.

In all the curve models (cf. the above) that we consider there is an immediate connection between $\mathbb{F}_q$-rational points on the Kummer line K_E of E, and $\mathbb{F}_q$-rational points of E and E^t. As such, when thinking about Kummer lines it is natural not to distinguish these (i.e., to consider everything up to $\mathbb{F}_{q^2}$-isomorphism). As a result, although some maps may only be defined over $\mathbb{F}_{q^2}$, this will at most induce a twist. Since we are only concerned with the $\mathbb{F}_q$-rational points of the Kummer line, this is not an issue. In all that follows, we *could* easily make everything defined over $\mathbb{F}_q$, but as we shall see in Section 4 this may limit us when instantiating the Kummer lines (i.e., restrict us to *canonical* Kummer lines as opposed to *intermediate* or *squared*—see Section 3.2).

3 MAPS BETWEEN KUMMER LINES

In this section, we present the theoretical basis. We observe first that many Kummer lines have appeared in the literature; the work of Gaudry and Lubicz [2009] present the so-called *canonical* Kummer line, while Karati and Sarkar use[2] the *squared* Kummer line [Karati and Sarkar 2017b]. Moreover, there is the x-line of Montgomery curve (e.g., Curve25519 by Bernstein [2006a]) and the

[2]The formulas for this model had already appeared in the Explicit-Formulas Database [Bernstein and Lange 2015] referring to a discussion between Bernstein, Kohel, and Lange and contributing the main idea to Gaudry [2006].

y-line of a (twisted) Edwards curve [Castryck et al. 2008; Farashahi and Hosseini 2017]. It is not immediately clear how these are all connected; in particular, the relation between the (canonical and squared) Kummer lines and Montgomery and (twisted) Edwards curves is not clear. Though a recent paper by Karati and Sarkar [2017a] provides some connections, this is not completely satisfying. For instance, it relies on having rational points or using 2-isogeny, and does not give a unique connection.

In this section, we settle this and, in essence, show that they are all the same up to isomorphism. These isomorphisms are natural and simple (including computationally) and lead to natural connections between all the above Kummer lines. The core is summarized in Theorem 3.4, and a more complete overview is shown in Appendix A.

3.1 Models with Rational 2-torsion

The canonical and squared Kummer lines are projections of curves that have full rational 2-torsion, which follows from their description via theta functions. As such, we shall always assume to have this. We begin by showing that this allows a nice parametrization of Montgomery curves.

Proposition 3.1. *Let k be a field such that $\mathrm{char}(k) \neq 2$ and let $(M_{A,B}, O_M)$ be a Montgomery curve with discriminant Δ_M such that $M_{A,B}[2] \subset M_{A,B}(k)$. Then there exist $a, b \in \bar{k}^*$ such that $ab(a^4 - b^4) \neq 0$ and $a^2/b^2 \in k$ such that*

$$A = -\frac{a^4 + b^4}{a^2 b^2}, \quad \Delta_M = 16B^6 \cdot \frac{(a^4 - b^4)^2}{a^4 b^4}.$$

Moreover, its points of order 2 are $(0 : 0 : 1)$, $(a^2 : 0 : b^2)$ and $(b^2 : 0 : a^2)$.

Proof. As $M_{A,B}[2] \subset M_{A,B}(k)$, the polynomial $x^2 + Ax + 1$ splits over k and thus $\sqrt{A^2 - 4} \in k$. Now fix any $b \in \bar{k}^*$ and take $a \in \bar{k}^*$ such that $a^2/b^2 = (\sqrt{A^2 - 4} - A)/2$. Note that $\sqrt{A^2 - 4} - A \neq 0, \pm 2$, because $\mathrm{char}(k) \neq 2$. Moreover $a^4 - b^4 = 0 \iff a^4/b^4 - 1 = 0 \iff a^2/b^2 = \pm 1$. Again, this is not possible, since $\mathrm{char}(k) \neq 2$. The statements for A, Δ_M and the 2-torsion points are simple calculations, recalling that M has discriminant $\Delta_M = 16B^6(A^2 - 4)$. □

For simplicity, we would like to have $B = 1$. Note that the curve $M_{A,B}$ is isomorphic to the curve $M_{A,1} : y^2 = x^3 + Ax^2 + x$ over $\bar{k}$, but not necessarily over k. Therefore, by making the assumption that $B = 1$, we are working *up to twist*. In what follows this shall not give rise to any issues, and as remarked earlier it does not impact the k-rational points of the Kummer line (even though it does change the k-rational points of the curve itself). So, from this point on, we consider

$$M/k : y^2 = x^3 - \frac{a^4 + b^4}{a^2 b^2} x^2 + x,$$

where $a, b \in \bar{k}^*$ such that $ab(a^4 - b^4) \neq 0$ and $a^2/b^2 \in k$.

Given this model, we can define a *dual* curve (which is *not* to be confused with the classical projective dual curve obtained as the set of tangent lines). For this purpose, we define $\hat{a}, \hat{b} \in \bar{k}^*$ such that

$$2\hat{a}^2 = a^2 + b^2, \quad 2\hat{b}^2 = a^2 - b^2.$$

It is easily checked that $\hat{a}^2/\hat{b}^2 \in k^*$ and that $\hat{a}\hat{b}(\hat{a}^4 - \hat{b}^4) \neq 0$. Therefore,

$$\widehat{M} : y^2 = x^3 - \frac{\hat{a}^4 + \hat{b}^4}{\hat{a}^2 \hat{b}^2} x^2 + x, \quad \Delta_{\widehat{M}} = 16 \cdot \frac{(\hat{a}^4 - \hat{b}^4)^2}{\hat{a}^4 \hat{b}^4}$$

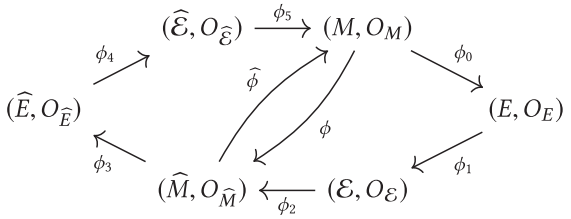
is a Montgomery curve whose elements of order 2 are $(0 : 0 : 1)$, $(\hat{a}^2 : 0 : \hat{b}^2)$ and $(\hat{b}^2 : 0 : \hat{a}^2)$. We call $\widehat{M}$ the *dual* of M. More generally, for any curve model, we call the action of swapping a (respectively, b) by $\hat{a}$ (respectively, $\hat{b}$) (and vice versa) *dualizing* (cf. Renes and Smith [2017, Section 4.1]).

The curves M and $\widehat{M}$ are 2-isogenous via a 2-isogeny $\phi : M \to \widehat{M}$, and the kernel of both ϕ and $\widehat{\phi}$ is generated by the point $(0 : 0 : 1)$ on the respective curves [Renes 2018, Remark 6]. This leads to a decomposition of the doubling map [2], which we use to construct the following sequence of maps. In more informal terms, each loop around the hexagon in Proposition 3.2 corresponds to a doubling operation on the Kummer line that was started from

Proposition 3.2. *Let $a, b \in \bar{k}^*$ with $ab(a^4 - b^4) \neq 0$ and $a^2/b^2 \in k^*$ and*

$$M/k : y^2 = x^3 - \frac{a^4 + b^4}{a^2 b^2} x^2 + x.$$

Then there exists a commutative diagram[3] of isogenies (over $\bar{k}$)



(3)

where

$$E/k : -x^2 + y^2 = 1 - \frac{(a^2 - b^2)^2}{(a^2 + b^2)^2} x^2 y^2, \quad \mathcal{E}/k : x^2 + y^2 = \frac{a^2 - b^2}{a^2 + b^2} \left(1 + x^2 y^2\right)$$

and $\widehat{E}$ and $\widehat{\mathcal{E}}$ are their respective duals. The maps ϕ_2 and ϕ_5 are 2-isogenies with

$$\ker(\phi_2) = \langle((0 : 1), (-\hat{b} : \hat{a}))\rangle, \quad \ker(\phi_5) = \langle((0 : 1), (-b : a))\rangle,$$

while the maps ϕ_0, ϕ_1, ϕ_3, and ϕ_4 are isomorphisms.

Proof. We define

$$\phi_0 : (x, y) \mapsto \left(\frac{2\hat{a}^2 x}{aby}, \frac{x + 1}{x - 1}\right), \quad \phi_0^{-1} : (x, y) \mapsto \left(\frac{y + 1}{y - 1}, \frac{2\hat{a}^2 (y + 1)}{abx(y - 1)}\right).$$

Note that this is *a priori* only a birational map, but naturally becomes an isomorphism when (canonically) extended to the smooth $\mathbb{P}^1 \times \mathbb{P}^1$ (or even $\mathbb{P}^3$) model—see, e.g., Silverman [2009], Proposition II.2.1. In particular, $\phi_0 : O_M \mapsto O_E, (0 : 0 : 1) \mapsto ((0 : 1), (-1 : 1))$. It is similar to the maps used by Bernstein et al. [2008, Theorem 3.2(i)] and by Castryck et al. [2008], but composed with the map by Hisil et al. [2008, Section 3.1] to ensure a twisted Edwards curve $E_{\alpha,\delta}$ with $\alpha = -1$ that is well-defined everywhere. Moreover, we tweak it such that it acts as an involution (i.e., a Hadamard transformation) on the Kummer lines. We define the isomorphism ϕ_1 as

$$\phi_1 : (x, y) \mapsto \left(-\frac{i\hat{b}}{\hat{a}} x, \frac{\hat{b}}{\hat{a}} y\right), \quad \phi_1^{-1} : (x, y) \mapsto \left(\frac{i\hat{a}}{\hat{b}} x, \frac{\hat{a}}{\hat{b}} y\right),$$

where $i \in \bar{k}$ is such that $i^2 = -1$. Then, we set $\phi_2 = \phi \circ \phi_0^{-1} \circ \phi_1^{-1}$. It follows that

$$\ker(\phi_2) = \langle \phi_1 \phi_0 (0, 0)\rangle = \langle((0 : 1), (-\hat{b} : \hat{a}))\rangle.$$

A completely analogous construction can be made for ϕ_3, ϕ_4, and ϕ_5. □

Remark 1. Note that one can argue that the above construction can be done for any sequence of isomorphisms starting at M. Indeed this is the case, but the above choice is a natural one and

[3]The diagram is drawn in the shape of a hexagon, because its induced diagram on the Kummer lines after translations by points of order 2 is the genus-1 analogue of the hexagon in genus 2 by Renes and Smith [2017, Figure 1].

gives rise to nice arithmetic on the Kummer lines. Moreover, it is a choice that allows us to explain the connection between Montgomery curves and the genus-1 Kummer lines arising from theta functions (i.e., Gaudry and Lubicz [2009], Section 6.2, and Karati and Sarkar [2017b], Section 2.4).

The maps behave very nicely on the Kummer lines.

Corollary 3.3. *There is an induced commutative diagram of Kummer lines*

$$\begin{array}{ccccc} & K_{\widehat{\mathcal{E}}}^{O_{\widehat{\mathcal{E}}}} & \xrightarrow{\bar{\phi}_5} & K_M^{O_M} & \\ \overset{\bar{\phi}_4}{\nearrow} & & & & \overset{\bar{\phi}_0}{\searrow} \\ K_{\widehat{E}}^{O_{\widehat{E}}} & & & & K_E^{O_E} \\ \underset{\bar{\phi}_3}{\nwarrow} & & & & \underset{\bar{\phi}_1}{\swarrow} \\ & K_{\widehat{M}}^{O_{\widehat{M}}} & \xleftarrow[\bar{\phi}_2]{} & K_{\mathcal{E}}^{O_{\mathcal{E}}} & \end{array} \tag{4}$$

such that

$$\begin{aligned} \bar{\phi}_0 &: (X : Z) \mapsto (X + Z : X - Z), \\ \bar{\phi}_1 &: (X : Z) \mapsto (\hat{b}X : \hat{a}Z), \\ \bar{\phi}_2 &: (X : Z) \mapsto (\hat{b}^2X^2 - \hat{a}^2Z^2 : \hat{a}^2X^2 - \hat{b}^2Z^2), \end{aligned}$$

while $\overline{\phi}_3 = \overline{\phi}_0$, *and* $\overline{\phi}_4$ *(respectively,* $\overline{\phi}_5$*) are obtained from* $\overline{\phi}_1$ *(respectively,* $\overline{\phi}_2$*) by dualizing.*

Proof. Apply the respective **x** and **y** projection maps to the curves in diagram (3). □

This provides clear connections between the x- and y- lines of Montgomery and (twisted) Edwards curves with full rational 2-torsion. We now show that we can use these 2-torsion points to obtain simple isomorphisms to the canonical and squared Kummer lines.

3.2 Actions of Points of Order 2

First recall from Section 2 that we have points of order 2

$$\begin{aligned} T &= (a^2 : 0 : b^2) \in (M, O_M), & \widehat{T} &= (\hat{a}^2 : 0 : \hat{b}^2) \in (\widehat{M}, O_{\widehat{M}}), \\ \Omega^+ &= ((1 : 0), (\hat{a}^2 : \hat{b}^2)) \in (E, O_E), & \widehat{\Omega}^+ &= ((1 : 0), (a^2 : b^2)) \in (\widehat{E}, O_{\widehat{E}}), \\ \Theta^+ &= ((1 : 0), (\hat{a} : \hat{b})) \in (\mathcal{E}, O_{\mathcal{E}}), & \widehat{\Theta}^+ &= ((1 : 0), (a : b)) \in (\widehat{\mathcal{E}}, O_{\widehat{\mathcal{E}}}). \end{aligned}$$

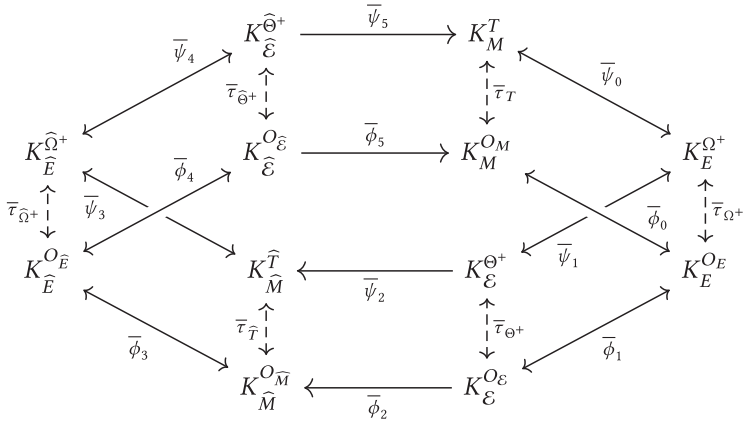
One can check that these are all respective images of one another under the ϕ_i. They correspond to translations[4] τ by the respective points that commute with the projection maps to $\mathbb{P}^1$. As a result, we obtain induced involutions $\overline{\tau}$ on the Kummer lines. More concretely, these involutions are

$$\begin{aligned} \overline{\tau}_T &: (X : Z) \mapsto (a^2X - b^2Z : b^2X - a^2Z), & \overline{\tau}_{\widehat{\Omega}^+} &: (X : Z) \mapsto (a^2Z : b^2X), \\ \overline{\tau}_{\widehat{T}} &: (X : Z) \mapsto (\hat{a}^2X - \hat{b}^2Z : \hat{b}^2X - \hat{a}^2Z), & \overline{\tau}_{\Theta^+} &: (X : Z) \mapsto (Z : X), \\ \overline{\tau}_{\Omega^+} &: (X : Z) \mapsto (\hat{a}^2Z : \hat{b}^2X), & \overline{\tau}_{\widehat{\Theta}^+} &: (X : Z) \mapsto (Z : X). \end{aligned}$$

Note that we could apply the maps τ to the diagram (3), but that requires keeping track of multiple coordinates and is somewhat tedious. Instead, for simplicity, we will focus on the Kummer lines. Applying the maps $\overline{\tau}$ to (4), we obtain the following result.

[4]Translations are morphisms [Silverman 2009, Theorem 3.6] and are therefore isogenies if and only if they send the base point of the domain curve to the base point of the co-domain curve. For example, $\tau_T : (M, O_M) \to (M, T)$ is an isogeny. As such, it is a group homomorphism.

Theorem 3.4. *The diagram*



is commutative, where

$$\overline{\psi}_0 : (X : Z) \mapsto (X + Z : X - Z), \qquad \overline{\psi}_3 : (X : Z) \mapsto (X + Z : X - Z),$$
$$\overline{\psi}_1 : (X : Z) \mapsto (\hat{b}X : \hat{a}Z), \qquad \overline{\psi}_4 : (X : Z) \mapsto (bX : aZ),$$
$$\overline{\psi}_2 : (X : Z) \mapsto (X^2 : Z^2), \qquad \overline{\psi}_5 : (X : Z) \mapsto (X^2 : Z^2),$$

and every $\mapsto$ is an isomorphism.

Proof. This is the diagram from (3) translated by corresponding points of order 2 through the different τ, projected to their respective Kummer lines. We construct

$$\overline{\psi}_0 = \overline{\tau}_{\Omega^+} \circ \overline{\phi}_0 \circ \overline{\tau}_T$$

and proceed similarly for the other $\overline{\psi}_i$. □

Recall that (the duals of) $K^{O_M}_M$, $K^{O_E}_E$ (respectively, $K^{O_{\mathcal{E}}}_{\mathcal{E}}$) are the Kummer lines of Montgomery, twisted Edwards, and Edwards curves, respectively. Hence, it remains to identify K^{T}_M, $K^{\Omega^+}_E$, and $K^{\Theta^+}_{\mathcal{E}}$ (and their duals). Since they are all simply $\mathbb{P}^1$ as an algebraic variety, we analyze their (pseudo-)addition formulae.

First note that Proposition 3.2 tells us that moving through the sequence $\overline{\phi}_0, \ldots, \overline{\phi}_5$ corresponds to the [2] map (starting at any of the $\overline{\phi}_i$). Since the $\overline{\tau}$ are isomorphisms, the same is true for $\overline{\psi}_0, \ldots, \overline{\psi}_5$. In other words, for example

$$[2] = \overline{\psi}_5 \circ \cdots \circ \overline{\psi}_0 \text{ on } K^{T}_M,$$
$$[2] = \overline{\psi}_4 \circ \cdots \circ \overline{\psi}_0 \circ \overline{\psi}_5 \text{ on } K^{\widehat{\Theta}^+}_{\widehat{\mathcal{E}}}.$$

Comparing these with the algorithm from Gaudry and Lubicz [2009, Section 6.2] (and the formulas also appear in Bernstein and Lange [2015]) reveals that these are the doubling formulae for the squared and canonical Kummer lines. One readily[5] verifies that the same is true for the differential addition formulae. The third Kummer line $K^{\Omega^+}_E$ has not appeared to our knowledge, and has similar arithmetic to the squared Kummer line. We refer to it as the *intermediate* Kummer, cf. Renes and

[5]This can be done by using the known addition formulae on the elliptic curves whose identities are at infinity, and composing with the translation and projection maps. This is somewhat tedious, but is relatively straightforward by using a computer algebra package [Bosma et al. 1997; The Sage Developers 2018].

Table 1. Kummer Lines over a Finite Field $\mathbb{F}_q$ and Their Associated (i) Squared Kummer $(a^2 : b^2)$ (ii) Montgomery A (iii) Twisted Edwards δ, and (iv) Edwards c^2 constants

q	$(a^2 : b^2)$	$(A : 1)$	$(\delta : 1)$	$(c^2 : 1)$
$2^{251} - 9$	(81 : 20)	(−6,961 : 1,620)	(−3,721 : 10,201)	(61 : 101)
$2^{251} - 9$	(186 : 175)	(−65,221 : 130,200)	(−121 : 130,221)	(11 : 361)
$2^{255} - 19$	(82 : 77)	(−12,653 : 6,314)	(−25 : 25,281)	(5 : 159)
$2^{266} - 3$	(260 : 139)	(−86,921 : 36,140)	(−14,641 : 159,201)	(121 : 399)

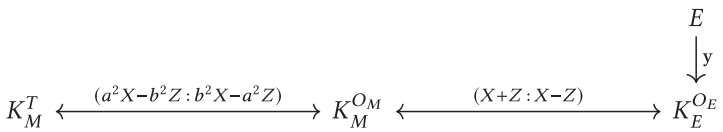


Fig. 1. The squared Kummer line, the x-line of a Montgomery curve, and the y-line of a twisted Edwards curve E, connected by involutions.

Smith [2017], Section 4.3. Interestingly, it appears as the y-line of a twisted Edwards curve where the coefficient of x^2 is -1, in which case the optimal formulas by Hisil et al. [2008] are available. For completeness, we summarize the associated curve constants for the instances provided by Karati and Sarkar in Table 1, connecting the squared Kummer line to the Kummer lines of Montgomery and twisted Edwards models via isomorphisms (as opposed to birational maps or isogenies).

Remark 2. We reiterate that only the intermediate Kummer line is new, while all the others have already appeared in the literature and are well-known. However, there had been little work in providing explicit maps between them, and this is exactly what we provide.

3.3 Hybrid Kummer Lines

Since the arithmetic on these Kummer lines is generally well-studied, the (cryptographic) value of this study does not come from improved operation counts. Beside its theoretical contribution, we ease the problem of selecting which curves to use for best performance (e.g., for standardization). That is, the simplicity of the isomorphisms gives quasi-cost-free transformations that allow interchangeable usage of any of the models. This is similar to the usage of a birational map to move between the Montgomery and twisted Edwards model, but we extend it with the squared Kummer line. We summarize this in Figure 1. In particular, Karati and Sarkar [2017b] show the benefits of the squared Kummer line on platforms where SIMD instructions are available.

Remark 3. Recall that all the above works under the assumption of having full rational 2-torsion. Although Montgomery and (twisted) Edwards curves always have a group order divisible by 4, it does not necessarily mean that they have full 2-torsion (i.e., they could have a point of order 4). Note that standardized curves such as Curve25519 and Curve448 do not have full 2-torsion, so this theory does not directly apply. More precisely, although all computations can still be performed, they are not guaranteed to be defined over the respective base fields $\mathbb{F}_{2^{255}-19}$ and $\mathbb{F}_{2^{448}-2^{224}-1}$.

Moreover, results from the well-studied Montgomery model immediately carry over to the squared Kummer line. For example, we can straightforwardly fit a (squared) Kummer line into the qDSA signature scheme. For signature verification, given $\mathbf{x}(P), \mathbf{x}(Q), \mathbf{x}(R) \in K_M^T$, we must be able to check whether $\mathbf{x}(R) = \mathbf{x}(P \pm Q)$. Although this can certainly be directly defined on K_M^T, we note that it is equivalent to checking whether

$$\overline{\tau}_T(\mathbf{x}(R)) = \overline{\tau}_T(\mathbf{x}(P \pm Q)).$$

Table 2. Comparison of an Implementation of the qDSA Signature Scheme Based on Curve25519 and the Montgomery Model of the Squared Kummer Line Defined by $(a^2, b^2) = (159, 5)$, Where the Memory is Measured in Bytes (B)

Ref.	Object	Constant	Clock cycles	Stack	Code
RS [2017]	Curve25519	$(A+2:4) =$ $(121{,}666:1)$	3,889,116 (sign) 6,793,695 (verify)	660 B 788 B	18, 443 B
This	$K_M^{O_M}$	$(A+2:4) =$ $(-5{,}929:795)$	3,916,879 (sign) 6,857,007 (verify)	660 B 788 B	18, 391 B
This	K_M^T	$(a^2:b^2) =$ $(159:5)$	3,824,857 (sign) 6,673,039 (verify)	660 B 788 B	18, 557 B

This is simply the function $\mathsf{Check}(\overline{\tau}_T(\mathbf{x}(P)), \overline{\tau}_T(\mathbf{x}(Q)), \overline{\tau}_T(\mathbf{x}(R)))$, where Check is defined in Renes and Smith [2017], Algorithm 2.

To demonstrate the feasibility of this approach, we extend the publicly available Curve25519-based instantiation of qDSA from Renes and Smith [2017] on the ARM Cortex M0 architecture.[6] For this purpose, we choose a squared Kummer line over $\mathbb{F}_{2^{255}-19}$, allowing field arithmetic to remain essentially unchanged. A notable exception to this is an efficient assembly implementation of 16×256-bit field multiplication, which is used for the multiplications by the line constants. This replaces the highly optimized multiplication by 121,666 from Düll et al. [2015]. We select $(a^2, b^2) = (159, 5)$, so that the squared Kummer line K_M^T corresponds to the *dual*[7] of `KL25519(82,77)` presented and implemented by Karati and Sarkar [2017b]. This implies the Montgomery constant of the curve above the line $K_M^{O_M}$ to be $(A+2:4) = (-5{,}929:795)$. We summarize the implementation results in Table 2. We emphasize that the point of this work is not to provide the most efficient implementation for this given platform, but rather to show the close connection between the different Kummer lines. Although on this platform results differ only by a minimal margin, the difference can be much larger on other devices (in particular, when SIMD instructions are available). Our isomorphisms allow an implementer to select the model that is most appropriate for a given architecture.

Remark 4. The implementations that we present are constant-time, and all standard countermeasures (e.g., projective blinding, scalar blinding [Coron 1999, Section 5]) against more advanced side-channel and fault attacks can be applied if required. In particular, as mentioned by the authors, the recent fault attack by Takahashi et al. [2018] can (cheaply) be thwarted by requiring nonces to be multiples of the cofactor (i.e., by "clamping"). However, such countermeasures are only necessary when an implementation is used in a context where fault attacks are considered part of the attacker model. We emphasize that our implementation is intended as a reference and *not* for production use.

4 ISOMORPHISM CLASSES OVER FINITE FIELDS

For cryptographic purposes, we are mostly concerned with the case that $k = \mathbb{F}_q$, for some prime (power) $q > 3$. As using extension fields is generally expensive, we would like to set things up such that all computation is performed in $\mathbb{F}_q$. Whether or not we can do this in a way such that constants remain small, depends on the number of Kummer lines that exist. Following earlier studies

[6] All code (including reference implementations in C) is available in the public domain at https://github.com/joostrenes/.

[7] The constants $(a^2, b^2) = (88, 77)$ lead to $(A+2:4) = (-25:25, 256)$, which has slightly larger constants on $K_M^{O_M}$ than its dual. However, results should be very similar.

on the number of isomorphism classes for certain curve models [Bernstein et al. 2008; Farashahi et al. 2012; Farashahi and Shparlinski 2010], we provide counts for the canonical, squared, and intermediate Kummer lines.

4.1 Identifying Kummer Lines

For this purpose it is interesting to ask when two Kummer lines should be considered to be the same. Given two Kummer lines $K_1 = E_1/\{\pm 1\}$ and $K_2 = E_2/\{\pm 1\}$ of elliptic curves E_1, E_2 defined over $\mathbb{F}_q$, it could be natural to identify K_1 with K_2 whenever E_1 is $\mathbb{F}_q$-isomorphic to E_2. However, as noted in Section 2, the arithmetic on the $\mathbb{F}_q$-rational points of the Kummer lines will be identical whenever E_1 is $\mathbb{F}_{q^2}$-isomorphic to E_2 (i.e., E_2 is the quadratic twist of E_1). The only twists that exist are quadratic, unless $j(E_1) \in \{0, 1728\}$, in which case, we may have higher order twists. We shall ignore this case in our analysis, which has only a very minor effect on our counts. As such, we can simply equate the number of Kummer lines with the number of elliptic curves defined over $\mathbb{F}_q$ up to $\bar{\mathbb{F}}_q$-isomorphism.

Recall that we parametrize Kummer lines by $a, b \in \bar{\mathbb{F}}_q$ such that $ab(a^4 - b^4) \neq 0$ and $a^2/b^2 \in \mathbb{F}_q$. Since $b \neq 0$, a Kummer line is defined by the fraction a/b or, equivalently, by the point $(a : b) \in \mathbb{P}^1$. Again, since $b \neq 0$, we can therefore simply assume $b = 1$. As such, we can consider $a \in \bar{\mathbb{F}}_q$ such that $a^2 \in \mathbb{F}_q$ and $a^5 - a \neq 0$.

4.2 Canonical Kummer Lines

We begin by considering the canonical Kummer line from Gaudry and Lubicz [2009] defined by some a as above. Recall that it corresponds to the y-line of the curve

$$\widehat{\mathcal{E}}/\mathbb{F}_q : x^2 + y^2 = \frac{1}{a^2}\left(1 + x^2y^2\right).$$

with identity $\widehat{\Omega}^+ = ((1 : 0), (a : 1))$, whose image in $\mathbb{P}^1$ is $(a : 1)$. Therefore, we require that $a \in \mathbb{F}_q$. It is easily seen that $\hat{a}^2, \hat{b}^2 \in \mathbb{F}_q$ and that this is enough to perform all arithmetic with $\mathbb{F}_q$ operations.

Now note that $(\widehat{\mathcal{E}}, \widehat{\Omega}^+)$ is $\mathbb{F}_q$-isomorphic to $(\widehat{\mathcal{E}}, O_{\widehat{\mathcal{E}}})$ via $\tau_{\widehat{\Omega}^+}$, which is an Edwards curve if and only if $a \in \mathbb{F}_q$ and $1/a^5 \neq 1/a$. The first is true by assumption, while the latter follows from $a^5 \neq a$. Therefore, we simply count the number of Edwards curves defined over $\mathbb{F}_q$ up to $\bar{\mathbb{F}}_q$-isomorphism. A result by Farashahi and Shparlinski [2010, Theorem 5] shows that the number of isomorphism classes is exactly

$$\begin{cases} \left\lfloor \dfrac{q+23}{24} \right\rfloor & \text{if } q \equiv 1, 9, 13, 17 \pmod{24}, \\ \left\lfloor \dfrac{q-5}{24} \right\rfloor & \text{if } q \equiv 5 \pmod{24}, \\ \left\lfloor \dfrac{q+1}{8} \right\rfloor & \text{if } q \equiv 3 \pmod{4}. \end{cases}$$

Thus, in general there will be no problem to find Kummer lines with the desired security properties. However, it may not be easy to find them such that its constants are small. For that reason, we look towards the squared and intermediate Kummer lines.

4.3 Squared and Intermediate Kummer Lines

If we use canonical Kummer lines, then we restrict ourselves to $a \in \mathbb{F}_q$ for all of the arithmetic to be in $\mathbb{F}_q$. This (seemingly) limits the number of Kummer lines that we can use. This is no longer the case on squared and intermediate Kummer lines; it suffices to only have $a^2 \in \mathbb{F}_q$. Note that this implies that $a \in \mathbb{F}_{q^2}$.

Since the j-invariants of M, E, and $\mathcal{E}$ and their duals are all equal, we can count the number of curves up to isomorphism of the form

$$\widehat{\mathcal{E}} : x^2 + y^2 = \frac{1}{a^2}\left(1 + x^2y^2\right)$$

such that $a^5 \neq a$ (but note that $\widehat{\mathcal{E}}$ is not necessarily an Edwards curve over $\mathbb{F}_q$). There are exactly $q - 3$ such curves, so it remains to determine how many are in the same $\bar{\mathbb{F}}_q$-isomorphism class. This question has already been considered by Edwards [2007, Proposition 6.1], whose statement implies that two Edwards curves determined by $a^2, \overline{a}^2 \in \mathbb{F}_q$ have the same j-invariant whenever $\overline{a}^2$ is one of the following:

$$\pm a^2, \pm \frac{1}{a^2}, \pm\left(\frac{a-1}{a+1}\right)^2, \pm\left(\frac{a+1}{a-1}\right)^2, \pm\left(\frac{a-i}{a+i}\right)^2, \pm\left(\frac{a+i}{a-i}\right)^2. \tag{5}$$

If $q \equiv 1 \pmod 4$, then $i^q = i$ and a straightforward computation show that

$$\pm\left(\frac{a-1}{a+1}\right)^2, \pm\left(\frac{a+1}{a-1}\right)^2, \pm\left(\frac{a-i}{a+i}\right)^2, \pm\left(\frac{a+i}{a-i}\right)^2 \in \mathbb{F}_q \iff a \in \mathbb{F}_q.$$

If $q \equiv 3 \pmod 4$, then $i^q = -i$ and a similar computation shows that

$$\pm\left(\frac{a-1}{a+1}\right)^2, \pm\left(\frac{a+1}{a-1}\right)^2 \in \mathbb{F}_q \iff a \in \mathbb{F}_q,$$
$$\pm\left(\frac{a-i}{a+i}\right)^2, \pm\left(\frac{a+i}{a-i}\right)^2 \in \mathbb{F}_q \iff i \cdot a \in \mathbb{F}_q.$$

Given that either $a \in \mathbb{F}_q$ or $i \cdot a \in \mathbb{F}_q$, while half the elements of $\mathbb{F}_q$ are squares, we closely approximate[8] that the number of isomorphism classes is

$$\approx \begin{cases} \left\lfloor \left(\frac{1}{4} + \frac{1}{12}\right)\frac{q}{2} \right\rfloor = \left\lfloor \frac{q}{6} \right\rfloor & \text{if } q \equiv 1 \pmod 4, \\ \left\lfloor \left(\frac{1}{8} + \frac{1}{8}\right)\frac{q}{2} \right\rfloor = \left\lfloor \frac{q}{8} \right\rfloor & \text{if } q \equiv 3 \pmod 4. \end{cases}$$

A more careful analysis (cf. Farashahi and Shparlinski [2010]) could be done, but such a close estimate suffices for our purposes. Interestingly, for $q \equiv 3 \pmod 4$ the number of canonical and squared Kummer lines is about the same. Thus, although $a^2 \in \mathbb{F}_q$ is a weaker restriction than $a \in \mathbb{F}_q$, it does not actually lead to more Kummer lines (up to isomorphism). This is explained by the fact that -1 is a non-square, since $q \equiv 3 \pmod 4$, hence exactly one of a^2 or $-a^2$ must be a square in $\mathbb{F}_q$, while their corresponding Edwards curves are isomorphic. For $q \equiv 1 \pmod 4$ there is a clear difference in the number of Kummer lines, so in that case there is a significant advantage in finding small parameters for a squared or intermediate Kummer line over a canonical Kummer line.

5 CONCLUSION

This article fills in the gaps between several existing results in the literature. We show that Kummer lines are very closely related to the traditional Montgomery and (twisted) Edwards models via translations by (rational) points of order 2. In particular, we demonstrate that the use of the cryptographically unconventional and sub-optimal Legendre model (as by, e.g., Karati and Sarkar [2017a] and Gaudry and Lubicz [2009]) is unnecessary and can be replaced by the arithmetically

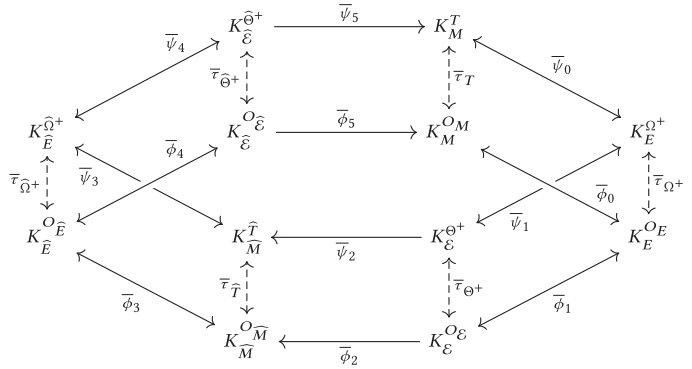
[8]This statement is exact up to the observation that some of the elements in (5) can be the same, which happens only exceptionally.

more efficient Montgomery and (twisted) Edwards models. Concretely, we provide the constants for these models for all Kummer lines appearing in the work of Karati and Sarkar [2017a] in Table 1 and work out simple and efficient maps to move between them in Theorem 3.4. These maps provide guidance for, and significantly simplify, the implementers' work. As an example, we provide details of an implementation of the qDSA signature scheme based on a squared Kummer line in Section 3.3.

APPENDIX

A GENUS 1 KUMMER ISOGENIES

In the maps below, $\overline{\tau}_T$, $\overline{\tau}_{\Omega^+}$, $\overline{\tau}_{\Theta^+}$, $\overline{\tau}_{\widehat{T}}$, $\overline{\tau}_{\widehat{\Omega}^+}$, $\overline{\tau}_{\widehat{\Theta}^+}$, $\bar{\phi}_0$, $\bar{\phi}_3$, $\overline{\psi}_0$, $\overline{\psi}_3$ are involutions; $\bar{\phi}_1$, $\bar{\phi}_4$, $\overline{\psi}_1$, $\overline{\psi}_4$ are isomorphisms; $\bar{\phi}_2$, $\bar{\phi}_5$, $\overline{\psi}_2$, $\overline{\psi}_5$ are 2-isogenies.



$(a^2 : b^2) = (\hat{a}^2 + \hat{b}^2 : \hat{a}^2 - \hat{b}^2) \in \mathbb{P}^1$

$M : y^2 = x^3 - \left((a^4 + b^4)/(a^2 b^2)\right) x^2 + x$

$E : -x^2 + y^2 = 1 - (\hat{b}^4/\hat{a}^4) x^2 y^2$

$\mathcal{E} : x^2 + y^2 = (\hat{b}^2/\hat{a}^2)\left(1 + x^2 y^2\right)$

$(\hat{a}^2 : \hat{b}^2) = (a^2 + b^2 : a^2 - b^2) \in \mathbb{P}^1$

$\widehat{M} : y^2 = x^3 - \left((\hat{a}^4 + \hat{b}^4)/(\hat{a}^2 \hat{b}^2)\right) x^2 + x$

$\widehat{E} : -x^2 + y^2 = 1 - (b^4/a^4) x^2 y^2$

$\widehat{\mathcal{E}} : x^2 + y^2 = (b^2/a^2)\left(1 + x^2 y^2\right)$

$O_M = (0 : 1 : 0)$, $T = (a^2 : 0 : b^2)$

$O_E = (0 : 0 : 1 : 1)$, $\Omega^+ = ((1 : 0), (\hat{a}^2 : \hat{b}^2))$

$O_{\mathcal{E}} = (0 : 0 : \hat{b} : \hat{a})$, $\Theta^+ = ((1 : 0), (\hat{a} : \hat{b}))$

$O_{\widehat{M}} = (0 : 1 : 0)$, $\widehat{T} = (\hat{a}^2 : 0 : \hat{b}^2)$

$O_{\widehat{E}} = (0 : 0 : 1 : 1)$, $\widehat{\Omega}^+ = ((1 : 0), (a^2 : b^2))$

$O_{\widehat{\mathcal{E}}} = (0 : 0 : b : a)$, $\widehat{\Theta}^+ = ((1 : 0), (a : b))$

$\overline{\tau}_T : (X : Z) \mapsto (a^2 X - b^2 Z : b^2 X - a^2 Z)$

$\overline{\tau}_{\Omega^+} : (X : Z) \mapsto (\hat{a}^2 Z : \hat{b}^2 X)$

$\overline{\tau}_{\Theta^+} : (X : Z) \mapsto (Z : X)$

$\overline{\tau}_{\widehat{T}} : (X : Z) \mapsto (\hat{a}^2 X - \hat{b}^2 Z : \hat{b}^2 X - \hat{a}^2 Z)$

$\overline{\tau}_{\widehat{\Omega}^+} : (X : Z) \mapsto (a^2 Z : b^2 X)$

$\overline{\tau}_{\widehat{\Theta}^+} : (X : Z) \mapsto (Z : X)$

$\mathbf{id}(K^{O_M}_{M}) = \mathbf{x}(O_M) = (1 : 0)$

$\mathbf{id}(K^{O_E}_{E}) = \mathbf{y}(O_E) = (1 : 1)$

$\mathbf{id}(K^{O_{\mathcal{E}}}_{\mathcal{E}}) = \mathbf{y}(O_{\mathcal{E}}) = (\hat{b} : \hat{a})$

$\mathbf{id}(K^{O_{\widehat{M}}}_{\widehat{M}}) = \mathbf{x}(O_{\widehat{M}}) = (1 : 0)$

$\mathbf{id}(K^{O_{\widehat{E}}}_{\widehat{E}}) = \mathbf{y}(O_{\widehat{E}}) = (1 : 1)$

$\mathbf{id}(K^{O_{\widehat{\mathcal{E}}}}_{\widehat{\mathcal{E}}}) = \mathbf{y}(O_{\widehat{\mathcal{E}}}) = (b : a)$

$\mathbf{id}(K^{T}_{M}) = \mathbf{x}(T) = (a^2 : b^2)$

$\mathbf{id}(K^{\Omega^+}_{E}) = \mathbf{y}(\Omega^+) = (\hat{a}^2 : \hat{b}^2)$

$\mathbf{id}(K^{\Theta^+}_{\mathcal{E}}) = \mathbf{y}(\Theta^+) = (\hat{a} : \hat{b})$

$\mathbf{id}(K^{\widehat{T}}_{\widehat{M}}) = \mathbf{x}(\widehat{T}) = (\hat{a}^2 : \hat{b}^2)$

$\mathbf{id}(K^{\widehat{\Omega}^+}_{\widehat{E}}) = \mathbf{y}(\widehat{\Omega}^+) = (a^2 : b^2)$

$\mathbf{id}(K^{\widehat{\Theta}^+}_{\widehat{\mathcal{E}}}) = \mathbf{y}(\widehat{\Theta}^+) = (a : b)$

$\bar{\phi}_0 : (X : Z) \mapsto (X + Z : X - Z)$

$\bar{\phi}_1 : (X : Z) \mapsto (\hat{b} X : \hat{a} Z)$

$\bar{\phi}_2 : (X : Z) \mapsto (\hat{b}^2 X^2 - \hat{a}^2 Z^2 : \hat{a}^2 X^2 - \hat{b}^2 Z^2)$

$\bar{\phi}_3 : (X : Z) \mapsto (X + Z : X - Z)$

$\bar{\phi}_4 : (X : Z) \mapsto (bX : aZ)$

$\bar{\phi}_5 : (X : Z) \mapsto (b^2 X^2 - a^2 Z^2 : a^2 X^2 - b^2 Z^2)$

$\overline{\psi}_0 : (X : Z) \mapsto (X + Z : X - Z)$

$\overline{\psi}_1 : (X : Z) \mapsto (\hat{b} X : \hat{a} Z)$

$\overline{\psi}_2 : (X : Z) \mapsto (X^2 : Z^2)$

$\overline{\psi}_3 : (X : Z) \mapsto (X + Z : X - Z)$

$\overline{\psi}_4 : (X : Z) \mapsto (bX : aZ)$

$\overline{\psi}_5 : (X : Z) \mapsto (X^2 : Z^2)$

In addition, we have, $\bar{\phi}_1^{-1} : (X : Z) \mapsto (\hat{a}X : \hat{b}Z)$, $\bar{\phi}_4^{-1} : (X : Z) \mapsto (aX : bZ)$, $\overline{\psi}_1^{-1} : (X : Z) \mapsto (\hat{a}X : \hat{b}Z)$, $\overline{\psi}_4^{-1} : (X : Z) \mapsto (aX : bZ)$.

REFERENCES

D. J. Bernstein. 2006a. Curve25519: New Diffie–Hellman speed records. In *Proceedings of the 9th International Conference on Theory and Practice of Public-Key Cryptography*. 207–228. DOI: https://doi.org/10.1007/11745853_14

D. J. Bernstein. 2006b. Elliptic vs. Hyperelliptic, part I. Talk at ECC (Slides retrieved from http://cr.yp.to/talks/2006.09.20/slides.pdf).

D. J. Bernstein, P. Birkner, M. Joye, T. Lange, and C. Peters. 2008. Twisted Edwards curves. In *Proceedings of the 1st International Conference on Cryptology in Africa (Lecture Notes in Computer Science)*, S. Vaudenay (Ed.), Vol. 5023. Springer, 389–405. DOI: https://doi.org/10.1007/978-3-540-68164-9_26

D. J. Bernstein, C. Chuengsatiansup, T. Lange, and P. Schwabe. 2014. Kummer strikes back: New DH speed records. In *Proceedings of the 20th International Conference on the Theory and Application of Cryptology and Information Security*, Palash Sarkar and Tetsu Iwata (Eds.). Springer Berlin, 317–337. DOI: https://doi.org/10.1007/978-3-662-45611-8_17

D. J. Bernstein and T. Lange. 2007. Faster addition and doubling on elliptic curves. In *Proceedings of the 13th International Conference on the Theory and Application of Cryptology and Information Security*. 29–50. DOI: https://doi.org/10.1007/978-3-540-76900-2_3

D. J. Bernstein and T. Lange. 2015. Explicit-Formulas Database. Retrieved from: http://hyperelliptic.org/EFD/g1p/auto-edwards-yzsquared.html.

W. Bosma, J. Cannon, and C. Playoust. 1997. The Magma algebra system. I. The user language. *J. Symbol. Comput.* 24, 3–4 (1997), 235–265. DOI: https://doi.org/10.1006/jsco.1996.0125

W. Castryck, S. D. Galbraith, and R. R. Farashahi. 2008. Efficient arithmetic on elliptic curves using a mixed Edwards-Montgomery representation. *Cryptology ePrint Archive, Report 2008/218*. Retrieved from: http://eprint.iacr.org/2008/218.

T. Chou. 2015. Sandy2x. Message on the curves mailing list at Retrieved from: https://moderncrypto.org/mail-archive/curves/2015/000637.html.

D. V. Chudnovsky and G. V. Chudnovsky. 1986. Sequences of numbers generated by addition in formal groups and new primality and factorization tests. *Adv. Appl. Math.* 7, 4 (1986), 385–434.

J. S. Coron. 1999. Resistance against differential power analysis for elliptic curve cryptosystems. In *Proceedings of the Cryptographic Hardware and Embedded Systems Conference (CHES'99)*, Çetin K. Koç and C. Paar (Eds.), Vol. 1717. 292–302.

C. Costello and P. Longa. 2015. Four$\mathbb{Q}$: Four-dimensional decompositions on a $\mathbb{Q}$-curve over the Mersenne prime. In *Proceedings of the 21st International Conference on the Theory and Application of Cryptology and Information Security*. 214–235. DOI: https://doi.org/10.1007/978-3-662-48797-6_10

W. Diffie and M. E. Hellman. 1976. New directions in cryptography. *IEEE Trans. Inform. Theor.* 22, 6 (1976), 644–654. DOI: https://doi.org/10.1109/TIT.1976.1055638

M. Düll, B. Haase, G. Hinterwälder, M. Hutter, C. Paar, A. H. Sánchez, and P. Schwabe. 2015. High-speed Curve25519 on 8-bit, 16-bit, and 32-bit microcontrollers. *Design, Codes and Cryptog.* 77, 2 (2015). Retrieved from: http://cryptojedi.org/papers/#mu25519.

H. M. Edwards. 2007. A normal form for elliptic curves. *Bull. Amer. Math. Soc.* 44, 3 (July 2007), 393–422.

R. R. Farashahi and S. G. Hosseini. 2017. Differential addition on twisted Edwards curves. In *Proceedings of the 22nd Australasian Conference on Information Security and Privacy (ACISP'17)*. 366–378. DOI: https://doi.org/10.1007/978-3-319-59870-3_21

R. R. Farashahi, D. Moody, and H. Wu. 2012. Isomorphism classes of Edwards curves over finite fields. *Finite Fields Their Appl.* 18, 3 (2012), 597–612. DOI: https://doi.org/10.1016/j.ffa.2011.12.004

R. R. Farashahi and I. E. Shparlinski. 2010. On the number of distinct elliptic curves in some families. *Des. Codes Cryptog.* 54, 1 (2010), 83–99. DOI: https://doi.org/10.1007/s10623-009-9310-2

A. Faz-Hernández and J. López. 2015. Fast implementation of Curve25519 using AVX2. In *Proceedings of the 4th International Conference on Cryptology and Information Security in Latin America*. 329–345. DOI: https://doi.org/10.1007/978-3-319-22174-8_18

S. D. Galbraith. 2012. *Mathematics of Public Key Cryptography*. Cambridge University Press. Retrieved from: https://www.math.auckland.ac.nz/ sgal018/crypto-book/crypto-book.html.

P. Gaudry. 2006. Variants of the Montgomery form based on theta functions. Retrieved from: http://www.fields.utoronto.ca/audio/06-07/number_theory/gaudry/.

P. Gaudry. 2007. Fast genus 2 arithmetic based on Theta functions. *J. Math. Cryptol.* 1, 3 (2007), 243–265.

P. Gaudry and D. Lubicz. 2009. The arithmetic of characteristic 2 Kummer surfaces and of elliptic Kummer lines. *Finite Fields Their Appl.* 15, 2 (2009), 246–260. DOI: https://doi.org/10.1016/j.ffa.2008.12.006

H. Hisil. 2010. *Elliptic Curves, Group Law, and Efficient Computation*. Ph.D. Dissertation. Queensland University of Technology.

H. Hisil, K. K. Wong, G. Carter, and E. Dawson. 2008. Twisted Edwards curves revisited. In *Proceedings of the International Conference on the Theory and Application of Cryptology and Information Security*, Josef Pieprzyk (Ed.). Springer Berlin, 326–343.

S. Karati and P. Sarkar. 2017a. Connecting Legendre with Kummer and Edwards. *Cryptology ePrint Archive, Report 2017/1205*. Retrieved from: https://eprint.iacr.org/2017/1205.

S. Karati and P. Sarkar. 2017b. Kummer for genus one over prime order fields. In *Proceedings of the 23rd International Conference on the Theory and Applications of Cryptology and Information Security*. 3–32. DOI: https://doi.org/10.1007/978-3-319-70697-9_1

N. Koblitz. 1987. Elliptic curve cryptosystems. *Math. Comp.* 48 (1987), 203–209.

V. Miller. 1986. Use of elliptic curves in cryptography. In *Proceedings of the International Conference on the Theory and Application of Cryptology and Information Security. Lecture Notes in Computer Science*, Vol. 218. Springer Berlin, 417–426.

P. L. Montgomery. 1987. Speeding the Pollard and elliptic curve methods of factorization. *Math. Comput.* 48, 177 (1987), 243–264.

J. Renes. 2018. Computing isogenies between Montgomery curves using the action of (0, 0). In *Proceedings of the International Conference on Post-Quantum Cryptography*. Lecture Notes in Computer Science, Vol. 10786. Springer, 229–247. Retrieved from: https://ia.cr/2017/1198.

J. Renes and B. Smith. 2017. qDSA: Small and secure digital signatures with curve-based Diffie–Hellman key pairs. In *Proceedings of the 23rd International Conference on the Theory and Applications of Cryptology and Information Security*, Tsuyoshi Takagi and Thomas Peyrin (Eds.). Springer International Publishing, 273–302. DOI: https://doi.org/10.1007/978-3-319-70697-9_10

J. H. Silverman. 2009. *The Arithmetic of Elliptic Curves, 2nd Edition*. Springer. Retrieved from: http://link.springer.com/book/10.1007%2F978-0-387-09494-6.

A. Takahashi, M. Tibouchi, and M. Abe. 2018. New Bleichenbacher Records: Practical Fault Attacks on qDSA Signatures. *Cryptology ePrint Archive, Report 2018/396*. Retrieved from: https://eprint.iacr.org/2018/396.

The Sage Developers. 2018. *SageMath, the Sage Mathematics Software System (version 8.1)*. Retrieved from: https://sagemath.org.

Received January 2019; revised August 2019; accepted September 2019